A Method and System for Secure Wireless Database Management

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims the benefit of U.S. Provisional Patent Application Serial No. 60/247,523, filed on November 9, 2000.

FIELD OF THE INVENTION

The present invention generally relates to a method for maintaining the security of data transferred within a wireless database management system (WDMS), and relates more specifically to a method practiced by software implemented on a plurality of wireless devices and on a plurality of networked computers that comprise the WDMS.

BACKGROUND OF THE INVENTION

Security has become a high priority now that access to many computer systems is not physically limited to hard-wired networks. In the past, database administrators were forced to work within the confines of secure office computers or secure office computer networks that allowed access to a database, or its database management software. A WDMS allows the database administrator to monitor and manage the database remotely. If the database administrator does not happen to be physically near in the event of a crisis, then remote access translates directly into a quicker response and less downtime. This is extremely valuable to

companies, such as banks, auction houses, brokerage firms, etc., which must keep their databases running uninterrupted in order to prevent a loss of revenue.

Although a WDMS solves many problems, it introduces its own unique problem: how can the data transferred within the WDMS be kept secure? In the present state of the art in wireless communications, information is transmitted to and from a wireless device by electromagnetic radiation that will inevitably travel through public spaces. Obviously, it is not desirable, and in some cases it may be a violation of law, for a company to allow public access to the information kept in its databases. In addition, typically data must be transferred between a database server and a web or application server before it can be broadcast to a wireless device. These connections must also be secured in order to prevent unauthorized access to a WDMS. Without a proper method for securing data transferred within a WDMS, private and confidential information kept in a database or databases within it may become accessible to competitors or the criminal element, with a loss of revenue potentially resulting.

The need for securing data within a computer network is not new, and many security methods have been developed for keeping data secure within a computer network. At present, some of these methods are being adapted for use in less conventional computing environments such as wireless local area networks or wireless phone networks. However, heretofore there has been no system developed to address the unique and important security concerns of a WDMS. Such a system has its own special challenges that need to be understood and addressed. The need exists for a comprehensive method of securing data transmissions within and access to a WDMS.

SUMMARY OF THE INVENTION

The present invention provides a method for maintaining the security of communications within a wireless database management system. In transfer through a WDMS, data might be exchanged between hundreds of computers. The WDMS might comprise a wireless device, wireless base station, wireless proxy server, a plurality of routers and servers that make up the Internet, a web or application server, database server, and one or more databases. The medium, connection, and protocol used with each of these devices is different and each may present a different kind of security risk. In order to reduce the risk of data transferred within the WDMS being intercepted or captured, all the communications between these computers and their interconnections must be secured, preferably with several layers of security.

Using software that is implemented on a wireless device and a wireless base station, data transmitted and received by radio frequency between a wireless device and a wireless base station is encrypted using a private key method such as the Data Encryption Standard (DES) or the Advanced Encryption Standard (AES). The same data is also encrypted using a public key method such as Elliptic Curve Cryptography (ECC) or Rivest-Shamir-Adleman (RSA). The use of public and private key methods together constitutes a more robust and flexible security design than either method could provide on its own.

Data transferred from a wireless base station, through a wireless proxy server and the Internet, to a web or application server is secured with a low-layer security protocol such as the Secure Sockets Layer (SSL) protocol or the Transport Layer Security (TLS) protocol. A wireless web or application server (usually part of a company's Intranet) might be further secured by the implementation of at least one firewall. The firewall might be used to restrict the

set of IP addresses that can be connected to the Intranet to the IP addresses of the wireless devices or of the wireless proxy servers.

Unfortunately, even if data transfer between a wireless device and a database server is completely secure it still might not be completely private. There remains the possibility that private information kept on the database or databases part of the WDMS might be accessed through a lost or stolen wireless device. The present invention also provides a novel method, comprising several steps, for reducing the risk of this kind of unauthorized access.

A first step in preventing unauthorized users from accessing a database through the WDMS involves the authentication of a user's identity. The present invention accomplishes authentication by requiring a user to "log in" to the WDMS with one or more user identification phrases and passwords. An unauthorized user that finds or steals a wireless device would be unable to access information kept in the database or databases without having the user identification phrases and passwords necessary to log in.

To prevent the still rarer chance that a wireless device could be lost or stolen while an authorized user was still logged into the WDMS, another step is used. In the present invention, software implemented on a web or application server sets an adjustable timeout for connections between that wireless device and the web or application server. After a certain amount of idle time or inactivity, which might be specified by the user, the wireless device will automatically log out from the WDMS. While this does not completely preclude unauthorized users from accessing the database or databases within the WDMS, it makes it much more difficult by requiring them to do so within a very short time frame set by the authorized user.

However, adding a timeout feature to a security scheme for wireless devices also presents a new challenge for a would-be developer of a WDMS: database users and administrators are

often many layers deep into a database while they are working. It is extremely inconvenient — if not impossible — for a user to have to navigate back through layer upon layer of a database after he or she has been disconnected. An accidental timeout, perhaps caused by a temporary loss of a wireless connection, might cost hours of work for a user of the WDMS, and could result in an unstable database system if the interruption occurred while changes to the database were not complete. The present invention presents a novel solution to this problem by uniquely identifying the connections ("sessions") maintained between a wireless device and a database server. According to one embodiment of the invention, sessions are uniquely identified with information that is stored on a web or application server. Session identification information is also called "session ID". After a user disconnects by a timeout or log out from a database server, he or she may reconnect to the same position within the database or databases by accessing the session information stored in the web or application server memory along with his or her session ID. When the connection is reestablished, the user is returned to the same position as before or, alternatively may be prompted with a choice for this option. This technique is also useful because the session IDs allow for more than one user to connect to the database or databases within the WDMS simultaneously. Session IDs allow database users and administrators to work more efficiently, while at the same time providing an additional layer of security for the WDMS.

To further secure the WDMS, the present invention allows users to be categorized into groups that might have different levels of access to the database, for example groups that have View-only access, groups that have View-and-change-display access, and groups that have Administrative access. An administrator of the WDMS would be able to monitor what sessions are active, allowing him or her to keep track of who is using the WDMS and what they are doing with it.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other objects, advantages and features of the present invention will be apparent from the following detailed description and the accompanying drawings, in which:

FIG. 1 is a block diagram of the overall structure of a wireless database management system in accordance with an embodiment of the present invention;

FIG. 2 is a block diagram of a typical client within a wireless database management system in accordance with an embodiment of the present invention;

FIG. 3 is a block diagram of a typical Virtual Private Network (VPN) client within a wireless database system in accordance with an embodiment of the present invention;

FIG. 4 is a block diagram of a typical Intranet within a wireless database management system in accordance with an embodiment of the present invention;

FIG. 5 is a block diagram of a typical Virtual Private Network (VPN) Intranet within a wireless database management system in accordance with an embodiment of the present invention;

FIG. 6 is a block diagram of wireless and network security protocols that are encountered as a query and response are transmitted and received between a database and a wireless device in accordance with an embodiment of the present invention; and

FIG. 7 is a flowchart that illustrates the control flow of steps performed by software implemented on a wireless device and server in handling idle connections in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

While the present invention is susceptible to various modifications and alternative forms, certain preferred embodiments are shown by way of example in the drawings and will be described in detail herein. It should be understood, however, that it is not intended to limit the invention to the particular forms described, but to the contrary, the invention is intended to cover all modifications, alternatives and equivalents falling within the spirit and scope of the invention defined by the appended claims.

In FIG. **1**, the overall structure of a WDMS according to one embodiment of the invention is shown schematically. In general, data transferred within the WDMS is transmitted and received through the Internet **70** (or a VPN Tunnel **75** within the Internet) between a client **15** (or VPN client **5**) and an Intranet **150** (or VPN Intranet **160**). FIG. **2** shows an embodiment of a typical client **15**, and FIG. **4** shows an embodiment of a typical Intranet **150**. The VPN client **5** and Intranet **160** are shown in an embodiment in FIG. **3** and **5** respectively, and will be discussed separately below.

At the most fundamental level, data transferred within the WDMS is transferred from a wireless device **10** in FIG. **2** to a database **200** in FIG. **4** or from a database **200** to a wireless device **10**. A description of the WDMS of the invention will begin with a wireless device **10**, and follow the path of data transmitted from a wireless device **10** to a database **200**. Reference will be made to FIG. **6** for a description of various encoding, encrypting, and translation performed on the data being transmitted and received between a wireless device **10** and a database **200**.

A wireless device **10** might comprise a personal digital assistant (PDA), cell phone, two-way pager or other similar device. Referring to FIG. **6**, data to be transferred from a wireless

device **10** to a wireless base station (**30** in FIG. **2**), is secured with a method comprising two steps. First, a database query **260** in FIG. **6**, is converted to HTML **270** and encrypted with a private key method **280** such as the Data Encryption Standard (DES), DES Extended (DESX), or the Advanced Encryption Standard (AES). Private key encryption is also known as symmetric or symmetrical encryption because both the transmitter and receiver must have the same encryption key in order to encrypt and decrypt data. In a second step, data is encrypted using a public key method **290** such as Elliptic Curve Cryptography (ECC). By analogy with private key encryption, public key encryption is also known as asymmetric or asymmetrical encryption because the transmitter and receiver can decrypt data with their own keys; the keys need not be, and usually are not, the same. According to one embodiment, public key encryption for data transferred between a wireless device **10** in FIG. **2** and a wireless base station **30** is provided by ECC, which may be performed, for example, by an Elliptic Curve Diffie-Hellman function. The private key used in the first step, which might be a DESX key, is renewed for every exchange of data between the client and the server. In another embodiment, the present device might secure data transferred between a wireless device and a wireless base station with a different combination of public and private key encryption steps.

The method of encryption described above prevents data from being intercepted or captured as it is transferred by radio frequency through spaces that may be public **310** in FIG. **6**. Before broadcast between a wireless device **10** in FIG. **2** and a wireless base station **30** the data may also be compressed and parsed into packets designed for low bandwidth wireless broadcast **300** in FIG. **6**. After broadcast, the data is recollected and decompressed **305** before any necessary decryption is performed.

While wireless communications are described herein by way of example as radio frequency communications, it should be understood that the invention is not limited to radio frequency electromagnetic radiation as a mode of wireless communication. Such wireless communication may utilize other frequencies of electromagnetic radiation such as x-ray, ultraviolet, visible, infrared or microwave. Wireless communication might also rely on other forms of transport such as statistical fluctuations in the average density of matter like acoustic or seismic waves. Even dynamically varying thermal gradients might be harnessed as a mode for wireless communication.

Wireless base stations are shown as **30** in FIG. **2**. A wireless base station might be part of a wireless network architecture such as MOBITEX or MOTIENT that uses digital packet-switching methods such as the Global System for Mobile Communication (GSM), Time Division Multiple Access (TDMA), or Code-Division Multiple Access (CDMA). In another embodiment, the wireless network architecture might be circuit-switched. A wireless base station **30** is connected through a physical cable **40** to a wireless proxy server **50**. Before transfer between a wireless base station and a wireless proxy server, data is again encrypted with public and private keys **320** in FIG. **6** and, according to one embodiment, is also secured for transfer with a low-layer security protocol such as the Secure Socket Layer (SSL) protocol **330**.

SSL was designed as an Internet security standard; it combines public and private key encryption methods in order to secure data transferred through the Internet. In an embodiment, SSL may require web or application servers to use public key encryption in the form of Certificate Authorities or digital signatures such as VERISIGN, which are public keys issued to web sites that have been researched by a third party and confirmed to be what they claim to be prior to their public key being issued. A wireless device **10** in FIG. **2** might have public keys for

one or more web or application servers **90** in FIG. **4** stored in memory for use in SSL. If information stored on a wireless device does not match what is known about a particular web or application server (that is connected to a wireless device through the Internet **70**) then the connection may be terminated. If the connection is not terminated, then a wireless device **10** might generate a private key to be shared between it and that web or application server **90**. Such a private key might be encrypted with the public key of that web or application server before being transferred through the Internet. After a web or application server has obtained the private key from a wireless device in this manner, the data transferred between them might be encrypted with that private key. In another embodiment, SSL might be implemented with a different combination of public and private key encryption methods.

In an embodiment of the system of the invention, there is a plurality of wireless base stations **30** in FIG. **2**, each providing wireless access to a different geographical region (also known as a cell). Each wireless base station **30** is connected to a wireless proxy server **50**.

According to one embodiment of the WDMS of the invention, a wireless proxy server **50** that is networked with the wireless base stations **30** is also connected to the Internet **70**. Data transferred through the Internet is secured by encryption with a low-layer security protocol such as the Secure Sockets Layer (SSL) protocol (**330** in FIG. **6**) or the Transport Layer Security (TLS) protocol; it might rely on an encryption algorithm such as RSA, ElGamal, RC4, or MD5. In an embodiment of the WDMS, data transferred from a wireless device **10** to the Internet **70** through a wireless proxy server **50** might also be converted from standard wireless protocols and languages such as WAP, WDP, and WML into protocols and languages that can be used with the Internet such as TCP/IP, HTTP, HTTPS, and HTML **270** in FIG. **6**.

Referring to FIG. **4**, data transferred from the Internet **70** to a web or application server **90** might pass through a firewall **80** implemented within an Intranet **150**. In an embodiment, the firewall might allow Internet access only through specific assigned ports, such as port 443 (not shown). In another embodiment, the firewall might restrict the Internet IP addresses that may access the web or application server **90** to the IP addresses of the wireless proxy server or servers **50** in FIG. **2**, effectively limiting access to wireless devices **10** connected to the WDMS through those proxy servers. Alternatively, the firewall might restrict the IP addresses that may access the web or application server to the IP addresses of each wireless device connected to the WDMS, allowing an even greater degree of control over access to the WDMS. In yet another embodiment, the WDMS might be further secured through the use of two firewalls in a so called "DMZ" configuration, with one firewall **80** in FIG. **4** between the Internet **70** and a web or application server **90**, and a second firewall (not shown in FIG. **4**) between a web or application server **90** and a database server **100**.

In the presently preferred embodiment of the WDMS, it is possible for a virtual private network (VPN) to provide additional security to data transferred between a VPN client **5** in FIG. **1** and a VPN Intranet **160**. FIG. **3** shows an embodiment of the detailed structure of a VPN client **5**, and FIG. **5** shows an embodiment of the detailed structure of a VPN Intranet. A VPN is implemented by limiting access to every computer or computer network intervening a wireless base station **30** in FIG. **3** and a web or application server **90** in FIG. **5**.

As illustrated, the main differences in the structure of a typical client as shown in FIG. **2** and a VPN client as shown in FIG. **3** are the VPN-controlled wireless proxy server **60** in FIG. **3** and the VPN Tunnel **75**. A wireless base station **30** might connect to a VPN-controlled wireless proxy server **60** rather than a standard wireless proxy server (**50** in FIG. **2**). The VPN-controlled

wireless proxy server might then connect to only certain VPN-controlled servers that are also connected to the Internet. The plurality of VPN-controlled Internet servers between a VPN-controlled proxy server **60** and a web or application server **90** in FIG. **5** is known as a VPN Tunnel **75**. Similarly, the main difference in the structure of a typical Intranet as shown in FIG. **4** and a VPN Intranet as shown in FIG. **5** is the VPN Tunnel **75**.

In an embodiment, the VPN does not allow users outside the WDMS to have any access to data transferred within the WDMS; they cannot inspect data within the WDMS and they cannot find out from whence data is transmitted or received — they cannot see the data at all.

According to one embodiment of the present invention, software on the web or application server (**90** in either FIG. **4** or **5**) encrypts or decrypts data transferred from a wireless proxy server through the Internet **330** in FIG. **6** and translates the data **350**, which might be a database query or a response to a database query, to or from a protocol or language used with networks like the Internet, such as HTTP or HTML, into or out of a protocol or language that can be used by a database server **100** in either FIG. **4** or **5** such as SQL.

Data transferred in the correct form to the database server **100** in either FIG. **4** or **5** is processed, the database or databases **200** connected to the database server are accessed, and then data is sent **350** and translated **360** from the server side to the client side following the reverse path shown by the arrows in FIG. **6**. The data transferred from the server side to the client side would be secured by a method comprising all of the steps previously mentioned.

In addition to the steps previously mentioned, there are other steps that might be taken in securing data transferred within the WDMS. Software on a web or application server **90** in either FIG. **4** or **5** and software on a wireless device **10** in either FIG. **2** or **3** work together to perform a timeout function for connections maintained between a wireless device and a database

server **100** in either FIG. **4** or **5**. FIG. **7** shows more specifically how the user of the wireless device selects a period of time after which the connection between the wireless device and the database server is terminated if the wireless device remains idle (i.e., if it does not send any data to the database server). As described previously, this security measure would make it more difficult for someone other than the intended user of the WDMS to use it, for example, through a lost or stolen wireless device. Unless unauthorized users can find or steal a wireless device in less than the timeout period they cannot access data kept within the WDMS. Part **A** of FIG. **7** shows how a user of a wireless device **10** establishes a new connection or "session" with a database or databases through a web or application server.

After prompting from a user **400** software on the web or application server assigns session information **410** ("session ID"). The session ID is particularly useful within the system of the invention because it allows a user to reconnect to a session that was timed out as described above. As shown in Part **D** of FIG. 7, to reconnect to a previous session a user of a wireless device **10** need only make a request for that session **470**, whereupon a web or application server **90** would reply **480** by reconnecting the user to the WDMS. This could potentially save hours of the user's time by allowing him or her to reconnect directly to the same point within the database at which he or she was working before his or her connection timed out. Databases often have many different layers that must be navigated in order to find a particular piece of information. Also, a search done slightly differently on the same database may return completely different results. Session IDs would be stored, along with other information about the user's session (e.g., stored results of requests which that user has made to a database or databases) in order to allow a user to quickly find the position that he or she had previously held within the database structure.

Part **B** of FIG. **7** shows how a user might adjust the period for timeouts within the system of the invention by setting a time to be kept in memory on a web or application server. Software on a web or application server **90** asks a user at its console **440** how long he or she expects to remain idle **420**. The user replies with a specific length of time beyond which they do not expect to remain idle **430**. To further remove the possibility of unwanted user access to the WDMS, users may only adjust the length of the timeout from a console **440** to a web or application server, the console being hard-wired to the web or application server; allowing such a change to be made from a wireless device might compromise the privacy of the entire WDMS.

Part **C** of FIG. **7** shows how a web or application server **90** might repetitively check **450** how long a session has been inactive in order to ascertain whether or not it needs to be disconnected; if the session extends beyond the time limit set (by a user as shown in FIG. **7** part **B**) the user is disconnected and must either reestablish the connection or start a new connection. According to one embodiment of the present invention, stored results of user requests associated with a session ID are periodically erased from memory on the web or application server. A user of the WDMS determines how often the session IDs and the information associated with them is erased.

In another embodiment, the session IDs allow the user acting as administrator of the WDMS to keep track of how many users are currently logged on to the WDMS, and what requests those users are making of the database or databases connected to the WDMS. Effectively, this allows the additional step of intelligent human scrutiny to be added to the present security method.

In another embodiment of the present invention, the identity of an intended user of the WDMS might be authenticated by software implemented on a wireless device, on a web or

application server, or on a database server. For example, authentication of user identity might be made possible by demanding that users enter one or more user names and passwords for access to the WDMS. If user identification phrases and passwords are kept private, then unwanted user access is further limited.

In yet another embodiment of the present invention, additional security might be afforded to the WDMS by categorizing users into groups that have different levels of access to the database server. Table 1 shows an embodiment of how these categories might be organized.

Table 1: Categories for user access

CATEGORY	ACCESS ALLOWED
View-only access	Users may only view data kept in a database or databases.
View-and-change-display access	Users may view data kept in a database or databases, or may modify the format in which data is displayed.
Administrative access	Users may view or modify the format of data kept in a database or databases, and may manage the access of other users to a database or databases.

One group might be enabled only to view the data kept in the database (View-only access); another group might be able to both view the data kept in the database and modify the manner in which that data is displayed (View-and-change-display access); another group might have complete access to the database, being able to modify, view, or change the display of data

kept in the database, decide to what group other users might be assigned, and perform other administrative operations (Administrative access).

In still another embodiment of the present invention, user requests made to a database or databases from a wireless device may be assigned codes, which are in turn stored in a web or application server and associated with a particular session ID. By coding the user requests, data sent from a wireless device to a web or application server may be limited to a user request code and any necessary parameters that must accompany the particular request. Table **2** shows how, in one embodiment of the present invention, this step makes sending a full-text request from a wireless device to a web or application server unnecessary.

Table 2: Numbering user requests

CONVENTIONAL	**EFFICIENT WDMS**
"SELECT TABLE_NAME, INTIAL_EXTENT, NEXT_EXTENT, PCT_INCREASE, PCTUSED, PCTFREE, TABLESPACE_NAME, EXTENTS FROM DBA_TABLES WHERE OWNER=ERNIE"	"17ERNIE"

This step makes it unnecessary for queries to be sent more than once, saving time and rendering the information that might have been sent with the query unavailable to would be eavesdroppers.

As shown in FIG. **4** and **5**, in an embodiment of the present invention the WDMS includes a capacity for a user of a wireless device to connect to a plurality of database servers **100** and databases **200**. FIG. **4** and FIG. **5** do not show more than one database server, but in

another embodiment (not shown) one or more databases **200** might be connected a web or application server **90** by a different, separate database server. According to one embodiment of the invention, the addresses, which might be, for example, the IP addresses of each database server **100,** are stored on a web or application server **90**. Effectively, this allows a user of a single wireless device within the WDMS to access a plurality of databases by referring to the stored list of database server addresses.

In yet another embodiment, each database server's address is given a nickname that is stored along with it in the list of addresses on the web or application server. These nicknames are set by a user of the WDMS. For example, "MYBANK" can reference database "BANK" at IP address "207.208.77.99". A user of a wireless device refers to the nicknames of the databases that he or she accesses rather than the actual address; thus, an eavesdropper is unable to identify the addresses of the databases that he or she might be trying to gain access to illegally.

It should be understood that various changes and modifications to the presently preferred embodiments described herein would be apparent to those skilled in the art. Such changes and modifications may be made without departing from the spirit and scope of the present invention and without diminishing its attendant advantages.